DATA EXFILTRATION VIA PROXY

TCS Internal

Definition of Data Exfiltration

- A common data exfiltration definition is the theft or unauthorized removal or movement of any data from a device.
- Data exfiltration typically involves stealing data from personal or corporate devices, such as computers and cell phones, through various cyberattack methods.
- Another data exfiltration meaning is data exportation and extrusion, data leakage, or data theft, which can pose serious problems for organizations.
- Failing to control information security can lead to data loss that could cause reputational and financial damage to an organization.

TCS Internal

Event Name: UC002: Data Exfiltration via Proxy

Rule Description

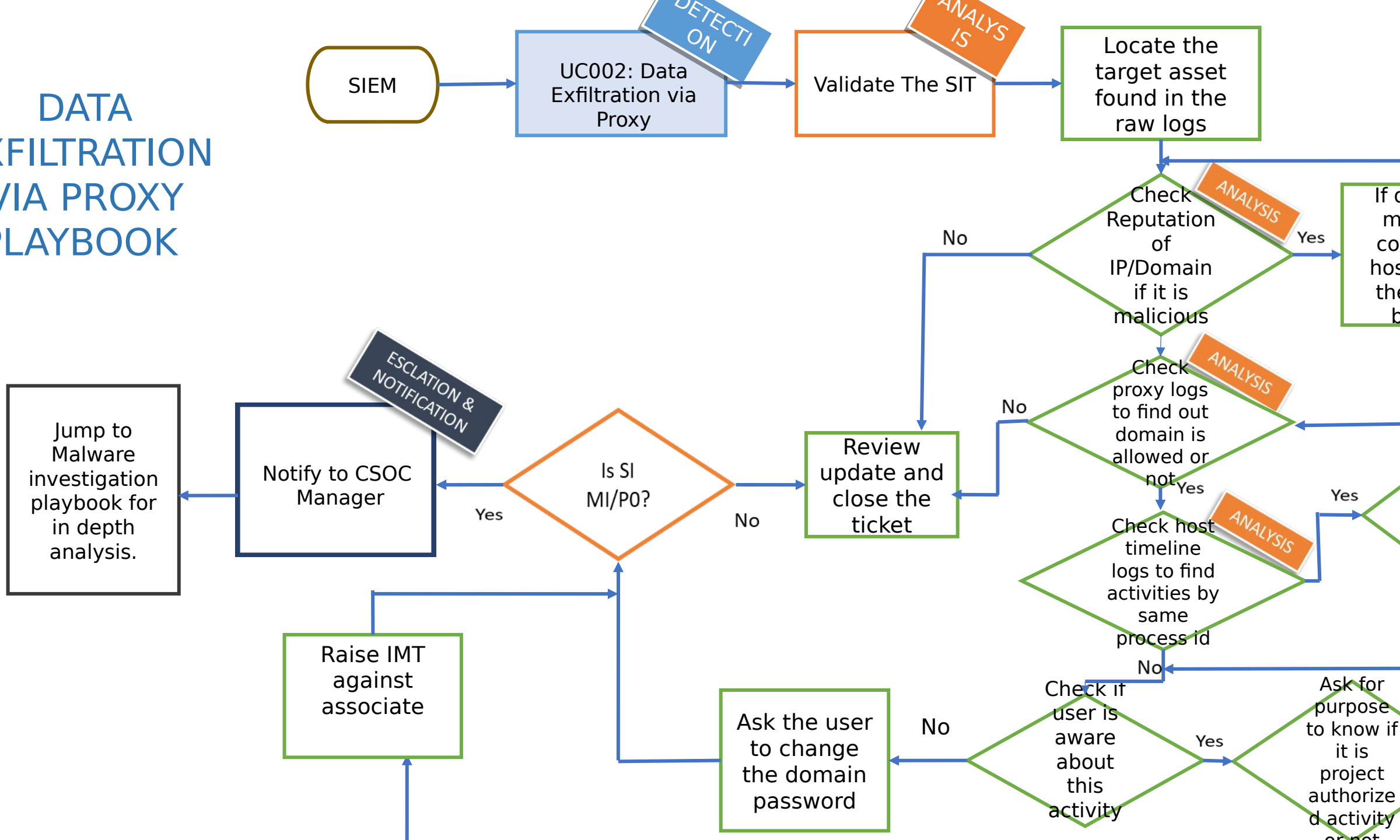
Apply UC002: Data Exfiltration via Proxy on events which are detected by the Local system
and when the event(s) were detected by one or more of **Blue Coat SG Appliance**
and when the event matches **web_Category (custom)** contains any of **[File Storage/Sharing or Peer-to-Peer or Software Downloads]**
and when the event matches **LONG("BC_BytesSent")>52428800** AQL filter query
and when an event matches any of the following **BB:Allowed proxy actions**
and NOT when any of URL (custom) are contained in any of **TCS_Exception_Data_Exfiltration - AlphaNumeric**

AQL or Ariel Query Language is used to to extract, filter, and perform actions on event and flow data that you extract from the Ariel database in IBM QRadar.

TCS Internal

Investigation Steps

1. Go through the events on Qradar console.
2. Locate the target asset mentioned in the raw logs.
3. Check the reputation of the Destination IP/Domain using reference of Who is , Recorded Future, IP Void, etc.
4. If the domain is malicious then contain the host and get the domain blocked on perimeter devices.
5. Check the proxy logs and verify if the attempts to this domain have been allowed or not.
6. Check host timeline logs to find activities by same process id and if yes also check if same process id has established some other domain and IP communications.
7. Check if user is aware about this activity and if yes ask for purpose for the same and understand if this is project authorized activity or not. Also ask the user to share ISM approval for the same. If the user does not have appropriate approval, raise an IMT against the user.
8. If the user is not aware about the activity, ask the user to change his domain password as a precautionary measure.
9. Check if the incident is P0 or related to any threat actors if yes then notify the CSOC Manager for the same. Also for further in-depth analysis kindly refer to Malware investigation playbook.
10. After this has been done you can go ahead and close the case.

TCS Internal

DATA EXFILTRATION VIA PROXY PLAYBOOK